# Simon Smith Investigator and Cyber Crime Expert discusses "Clone Websites"? on A Current Affair

**MELBOURNE, Australia - March 12, 2017** - *PRLog* -- **Simon Smith Investigator** - Note: The segment from 'A Current Affair' is at the end of this Press Release.

The episode featured Ann and discussed primarily the use of cloned websites, which is very similar to phishing (the use of email to pretend somebody is going to a real site).

Mr. Smith identified the IP, sent it to ACORN and stated, "ACORN have continuously failled both my customers and I many times, but this time I believe the bank has a duty of care to Ann, and as of the date of writing this release - of course ACORN have done nothing."

"Ann, who actually worked in finance, was manipulated by this fraudster and socially engineered and further harmed by what I consider 'negligent identity theft internet fraud', which the bank detection system aided the fraudster in allowing online", Mr. Smith said.

Mr. Smith tracked this permission based activity to India. The neglect did not end there it seems. "Due to a lack of police care, bank effort, and other crisis factors, including a lot of callouts and phone calls that wasted a lot of time, money and attention to the daily business, looking but not finding, valuable time was lost from the business, and other issues occured", Mr. Smith said.

He further stated, "GeneralIy without charging his client, the insurance company was so useless, they stated in their report that Ann should have taken the quote from the same 'IT guy' spending $2,000 on a 'firewall' router to replace her router. I was speechless. That is how stupid insurance companies are. A router is a firewall."

More losses followed. Mr. Smith was initially engaged to look into this fraud and did not have a lot of time allocated until instructed to pursue other issues the couple were enduring with their Companies, malware, loss of documents, data theft, and purported loss of paperwork and requests to look at stalking accusations.

Mr. Smith located the clone website, real name and they of course were just a victim too. It was another case of 'social engineering'. As Mr. Smith was only commissioned for a very short time on this task he was directed on other crisis matters for the couple. He was not asked to record any forensic reports - the purpose was to secure, fix and move on.

Mr. Smith stated, "Although I am 25 years beyond an IT person's job sadly Ann and her husband lived out in a country town and the way the entire IT network was set up was below acceptable standards and Ann could trust anyone. I explained to them that although faster, I am a higher level. They advised because their business ceased they needed me to perform this work NOW. I felt obligated on one side and sad on the other.".

"They really were not having a good time, that is really as far as it went, apart from being promised a full investigation from the bank which never happened. They lost primary sources of income from other forms of crisis that occured with their business which I detected on my own initiative, but nobody would help them", Mr. Smith stated.

Ann lost over $200,000 to fraudsters and what was not covered in the story was the bank's excuse that it somehow was all Ann's fault, a 65 year old lady. Mr. Smith spotted the banks public advertising stating

consumers are "not liable for the fraudulent or negligent conduct of '**the Bank**' staff or agents". Mr. Smith simply stated, "their security systems are in my expert opinion programmed to a level that is inferior and substandard.

They don't appear to detect a simple foreign IP address or spoofed request headers as a trigger which any other bank would immediately action. A monkey might as well have written them." If any lawyer would stand up and help Ann I would support them against the bank. This may be within VCAT's jurisdiction, so there would likely be no adverse costs.

Mr. Smith has succeeded in many investigations of fraud. Most of the time internet fraud is due to the "bank, based on a lack of due diligence and capacity to create a sophisticated algorithm that can analyze behavioural trends, request headers and recognise a simple offset trend to trigger an alert like every other bank does. He also said in his clients' experience a file with ACORN is like posting a letter to Santa".

Mr. Smith was appalled at what they did to Ann and stated, "They owe Ann a duty of care and they breached it. They promised her a call back and investigation more than 1.5 years ago and had the nerve to hang up on me with an authority to mediate. To this day, the shameless bank still has never called back."

**Mr. Smith will keep you posted on any developments if the bank does not rectify their error publically identifying them to Australia.**

*If you wish to check out Mr. Smith's profile, or wish to brief him on any Expert Witness or Cyber Investigation matters or make media contact please see below:*

**LinkedIn:** https://linkedin.com/in/simonsmithinvestigator/
**eVestigator:** http://www.evestigator.com.au
**Direct:** +61410643121 **Email:** forensic@evestigator.com.au
**Facebook:** www.facebook.com.au/evestigator
**Twitter:** www.twitter.com/e_forensic

https://youtu.be/tvjWLkf8YUI

--- End ---

| | |
|---|---|
| Source | Simon Smith eVestigator |
| Email | Click to contact author |
| Phone | +61410643121 |
| City/Town | Melbourne |
| State/Province | Victoria |
| Country | Australia |
| Industry | Banking |
| Tags | Simon Smith Investigator, eVestigator, Investigator |
| Link | https://prlog.org/12625867 |